AU/ACSC/2016

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

BATTLEFIELD OF THE FUTURE:

How to Achieve Superiority in the Cyberspace Domain

by

Dawn M. East, CIV, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Dr. Gregory F. Intoccia

Maxwell Air Force Base, Alabama

February 2016

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

TABLE OF CONTENTS

LIST OF FIGURES

ABSTRACT

The Cyberspace Domain is a relatively new and complex domain that interfaces with the other domains of air, land, sea, and space. The Department of Defense (DOD) released an introductory Strategy for Operating in Cyberspace in 2011, followed by an updated and more robust DOD Cyber Strategy in 2015. There are obvious shortcomings to both strategies; therefore this paper proposes how a revision of the current DOD cyber strategy will achieve an advantage against existing and near-term cyber threats. In order to assess what changes are necessary to achieve the kind of superiority contemplated by this paper, the following methodology is employed; the 2015 DOD cyber strategy is compared to the 2011 DOD cyber strategy; recommendations are made to show how the update is pertinent to the existing cyber posture. Key recommendations of the paper include how to identify and counter supply chain threats, as well as a strategy to define a cyber risk management plan that adheres to a set of standards put forth by the government. The paper recognizes a lack of private sector accountability and identifies how the DOD can assist the private sector and enforce accountability. The paper also endorses improvements to the rapid cyber acquisition cyber process and suggests how the DOD can improve the development and retention of an adequate cyber workforce.

INTRODUCTION

The Cyberspace domain is relatively new to the Department of Defense (DOD). Of the domains in which the military operates (Land, Air, Sea, Space and Cyberspace) Cyberspace has quickly gained significance as it has a pervasive reach in almost every aspect of DOD operations. This man-made domain has the capability to cripple or advance the ability for the U.S. to achieve superiority. Cyberspace superiority is defined as the degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations of that force, and its related land, air, sea, and space forces at a given time and sphere of operations without prohibitive interference by an adversary.[1]

Cyberspace is also readily available as a tool for adversaries that have traditionally been a huge threat and those that have only recently started taking advantage of the ease and accessibility of cyberspace to increase their chances of causing damage, infiltrating systems, or hindering operations. Both state and non-state actors are launching an increasing number of cyberattacks, using them as a political instrument in direct and non-direct ways. Conducting cyberattacks is a relatively inexpensive endeavor with potential for high yield effects and no attribution.[2] As such, the DOD has realized the need for dedicated strategy to deal with this newest and least understood domain of warfare. Unfortunately, any strategy put in place would prove short lived with the rapid advancement, sophistication and unpredictability of adversarial attacks and capabilities.

How can the current DOD cyber strategy be further revised to achieve an advantage against existing and near-term cyber threats? In order to achieve an advantage in cybersecurity, the DOD cyber strategy must acknowledge the rapidness in which technology proliferates, and

lend itself towards being dynamic to future changes. The DOD must also address supply chain threats and provide guidance for private sector accountability. It must focus on rapid cyber acquisition to stay abreast of current and emerging threats and also formally define a cyber risk management plan to properly mitigate all anticipated cyber threats. Lastly, it must implement a plan to recruit and retain a reliable cyber workforce that is dedicated to the cyber mission.

By critiquing the previous strategies, determining strengths and weaknesses, and highlighting the improvements from the 2011 to the 2015 DOD cyber strategy, one can obtain a clearer understanding of inclusion necessities in a new strategy. As predicted, the 2015 DOD cyber strategy is not flawless and will still call for modification to close gaps that have not been considered or are not yet addressed. The DOD must expand its efforts to build and maintain capabilities to conduct cyberspace operations, including increasing offensive cyber capabilities. It will attain achievement by identifying, obtaining and utilizing the rapidly advancing technologies that are readily available and soon to be released. It is important to understand the rapidly changing cyber environment and that the strategy must be dynamic and consistently updated to stay relevant.

This research paper is a fusion of the problem/solution and evaluation frameworks to scrutinize both the 2011 and 2015 DOD cyber strategies in order to make supplementary recommendations and updates. To assess what changes are necessary to achieve the kind of superiority contemplated by this paper, the following methodology is employed, the 2015 DOD cyber strategy is compared to the 2011 DOD cyber strategy; enhancements are addressed to show how the update is relevant to the current cyber posture. Statistical data from secondary sources such as the United States Government Accountability Office (GAO) Reports to Congressional Committees provides applicable data on the past and current cyber posture, and is

suitable to forecast future trends in the cyber domain. The GAO reports are germane to the topic in that the data trends will show the impact that both the 2011 and 2015 strategies had through actual cyber threats and incidents.

Following this methodology, the paper intends to examine the DOD Strategy for Operating in Cyberspace (May 2011) and identify shortcomings and/or weaknesses. There is then an associated analysis of the DOD Cyber Strategy (April 2015) with a discussion on improvements and significant updates. The frame of reference for determine the shortcomings and/or weaknesses of these strategies is a combination of personal expertise, industry experts, and a breakdown of how the strategic initiatives and goals fail to directly respond to specific threats and types of exploits. Finally, the research paper will propose updates to the cyber security strategy based off the inadequacies in the 2015 DOD cyber strategy.

BACKGROUND

Before critiquing the 2011 and 2015 DOD cyber strategies, it is important to present background information to show why these strategies are so important, and why the 2015 DOD cyber strategy requires further revision. This section starts with an overview of the current DOD cyber posture. The overview includes the current collaborative efforts in which DOD participates, as well as a brief description of some of the most critical threat types that are present today. Descriptions of common threat sources and types of exploits that are most typical are given. This section also provides some statistics on number of attacks and whom they affected. Lastly, background information on commercial and industry involvement is included.

In the previous eight years, the number of information security (IS) related incidents reported by federal agencies to the U.S. Computer Emergency Readiness Team (US-CERT) have increased from 5,503 to 67,168, an increase of 1,121 percent.[3] This rapid rise in incidents was one of the major catalysts that prompted the U.S. Government to take action and define a cyber security strategy. The DOD Strategy for Operating in Cyberspace to battle the IS related incidents was released in May 2011. Four years later, a modified and expanded DOD Cyber Strategy was released in April 2015 with the purpose of updating the previous strategy, given that the number of IS incidents continued to increase in frequency, and cyber technology was rapidly changing.

While the 2011 DOD cyber strategy guided the DOD's cyber activities and operations in support of United States national interests over the last four years, the current strategy sets prioritized strategic goals and objectives for DOD's cyber activities and missions to achieve over an undetermined amount of years. It concentrates on building capabilities for effective cyber security and cyber operations to defend DOD networks, systems, and information; to defend the nation against cyber-attacks of noteworthy consequence; and support operational and contingency plans. Lastly, it builds on preceding decisions regarding DOD's Cyber Mission Force and cyber workforce development and provides specific guidance to mitigate anticipated risks and capture opportunities to strengthen U.S. national security.[4]

Although the current DOD cyber strategy is only about a year old as of this writing, it still does not provide a comprehensive plan for existing and potential threats because the threats are constantly evolving and maturing. It is vital that the United States not only react to these threats, but also anticipate and mitigate them. Lt. Gen James Clapper, Jr., Director of National Intelligence believes that the most menacing foreign intelligence threats involve cyber-enabled

espionage, insider threats and espionage by China, Russia, and Iran.[5] His theory supports the current thinking on the matter by the DOD and other U.S. government agencies that there are three specific and unique threat types: supply chain, malicious insiders, and foreign actors. Unfortunately, due to shortcoming in the current policy, the current DOD cyber strategy cannot keep up with all of these threats. An analysis of both the 2011 and 2015 DOD cyber strategies could assist in building proposals, revisions and updates that will allow the DOD to achieve superiority in the cyber domain.

CURRENT DEPARTMENT OF DEFENSE (DOD) CYBER POSTURE

Collaboration

Collaborative efforts between the DOD and other U.S. government agencies are a large contributor to the success of the U.S. in cyber security. The DOD cyber strategy is only part of the bigger picture, in addition to operating on its own goals, due to its nature, the U.S. cyber strategy must take on a "whole-of-government" approach to defend against and respond to threats. This is a concept that would establish a unified effort between multiple government agencies in order to maximize all available resources through a collaborative effort. It requires the DOD to cooperate with agencies of the U.S. government, with the private sector, and with international partners to share information, build alliances, and foster norms of responsible behavior to improve global strategic stability.[6]

To this end, the Secretary of Defense directed the Commander of the United States Strategic Command to establish a sub-unified command of the United States Strategic Command (USSTRATCOM), United States Cyber Command (USCYBERCOM). Its mission is to plan,

coordinate, integrate, synchronize and conduct activities to: direct the operations of identified DOD information networks; and when directed, conduct full range military cyberspace operations to enable activities in all domains, and ensure U.S./Allied freedom of action in cyberspace while denying the same to adversaries.[7] This command has representation from all branches of the military; to include U.S. Army Cyber Command, the 24th Air Force, U.S. Coast Guard Cyber Command, U.S. Fleet Cyber Command/ U.S. 10th Fleet, and U.S. Marine Corps Forces Cyber Command.

Further partnerships include those with the National Security Agency (NSA), the Central Intelligence Agency (CIA), the Defense Advanced Research Projects Agency (DARPA), the Department of Homeland Security (DHS), and other public and private investments and initiatives. In addition, in Feb 2015 the President directed the Director of National Intelligence (DNI) to establish the Cyber Threat Intelligence Integration Center (CTIIC); this national intelligence center focuses on gathering and analyzing information regarding malicious foreign cyber threats to the nation and cyber incidents affecting U.S. national interests, and provides all-source analysis of threats to U.S. policymakers. It also assists relevant departments and agencies in their efforts to identify, investigate, and mitigate those threats.[8]

Both the 2011 and the 2015 DOD cyber strategies identify the need for collaboration by dedicating specific strategies and goals to working with additional government departments and agencies as well as U.S. allies and international partners. DHS is ultimately responsible for securing cyberspace at the national level, but all other government agencies and departments are responsible for securing the portions of cyberspace that lie under their authority; if one system is compromised it can have detrimental effects and negatively influence other organizations.

Types of Threats

Although the DOD mission is susceptible to a variety of cyberattacks, there is a categorization of three specific and unique types: supply chain, malicious insiders, and foreign actors. These threat types must be understood in order to have a strategy that is equipped to combat the specific damages that they can cause. According to Cyber Vision 2025, the threat types are described in further detail below.[9]

The supply chain threat focuses on the flow of products that go from the production source to the end user and the opportunities for attack during both the movement and manufacturing of these products. The supply chain is complex and provides many opportunities for those with malicious intent to infiltrate and potentially contaminate critical components of cyber related products, particularly in the manufacturing phase. During this phase, an adversary has the ability to take steps that ultimately allow access to computer systems, gather sensitive information, or disrupt computer operations through the use of sub-standard, malicious or counterfeit IT components and software. Supply Chain Risk Management (SCRM) is increasingly important in the acquisition of new cyber products and is now taken into account and tracked in this process. Finding a balance between a secure mixing of government off the shelf (GOTS) and commercial off the shelf (COTS) components for cyber systems is critical.

The malicious insider threat includes both willing and unknowing participants. The willing participants are motivated by a number of different factors; having legitimate access to information systems provides an opportunity to input corrupt data or malicious software into critical missions systems. Recent media exposure of malicious government employees and contractors has shown that people are willing to compromise systems and information. Further,

unknowing participants unintentionally enable or create cyber vulnerabilities through bad information assurance practices or lack of operational security measures.

The foreign actor threat describes actors that have the capability and intent to leverage threats to exfiltrate strategically, operationally and/or tactically relevant data and launch persistent cyberattacks. The foreign threat ties into the supply chain threat; circuit card components that are made in a foreign factory have an increased opportunity for insertion of compromised parts with unintentional functions or software.

Threat Sources and Types of Exploits

Not only does the DOD and the entire United States face cyber threats from different adversaries, but the types of threats are widely varied. Adversaries fluctuate in terms of their capabilities, inclination to act, and motivations, which include seeking financial gain or a political, economic, or military advantage.[10] There are common cyber adversaries that make up a detailed list of threat sourced as well as types of exploits that are typical of adversaries, both state and non-state. Details on the threat sources and types of exploits below are cited from the GAO report, *Information Security Cyber Threats and Data Breaches Illustrate Need for Stronger Controls across Federal Agencies*.[11]

Bot-network operators use a network of compromised remotely controlled systems to coordinate attacks and distribute phishing schemes, spam, and malware attacks, without the knowledge of the user or host. Some of these network services are available in underground markets. Financial gain is a motivator for criminal groups pursing attacks on systems; they use cyber exploits for stealing identities, computer fraud, and internet extortion. International

corporate spies and criminals also pose a threat to the U.S. through the ability to organize monetary theft in large amounts, industrial espionage, and to employ or mature hacker talent.

Hackers break into networks for a number of reasons, including the challenge, annoyance, payback, or to earn large amounts of money. It once took a good amount of computer knowledge or skills to gain unauthorized access, Hackers can download attack scripts and protocols to gain unauthorized access rather easily, even without a large amount of computer knowledge or skills. This means that although these implements have become more refined, they have also become simpler to use. Most hackers do not have the obligatory know-how to credibly threaten challenging marks (such as critical U.S. networks), but the international populace of hackers poses a comparatively high risk of an isolated or momentary disruption, triggering grave damage.

Employees that are dissatisfied in their job make up the primary basis of insider computer crime. They do not need to possess a great amount of system or network intrusion knowledge based on their rank within the company – which allows them unhampered access to cause damage to a system or to steal sensitive data. The insider threat includes indifferent or badly trained employees who can unintentionally insert malware into systems and networks

Nations use cyber tools as part of data collecting and espionage actions. Quite a few nations are working to improve information warfare guidelines, platforms and proficiencies. This empowers an individual to possibly have a grave and momentous impact by disturbing supply, communications, and economic infrastructures that maintain military authority. Adversaries look for means to debilitate, terminate, or exploit critical infrastructures in order to threaten national security, ensure mass casualties, deteriorate the economy, and harm public morale and assurance.

Adversaries could also use phishing techniques or spyware/malware in order to collect money or obtain sensitive data.

The threat sources identified above take advantage of several exploits to unfavorably distress systems, networks and operations. Some are identified below. Cross-site scripting takes advantage of third-party resources to run script inside the target's web browser application. This technique exploits weaknesses that allow an attacker to steal cookies, take screen images, record key strokes, identify and gather network information, and gain access to control the victim's machine from another location.

Denial-of-service thwarts approved users of networks and systems from opening them by draining resources. A similar type of attack is distributed denial-of-service in which numerous hosts accomplish the attack. Malware is a program injected into a system, typically without the owner's knowledge, set on weakening the integrity, confidentiality, or availability of the host's data, or otherwise aggravating or distracting them. Examples include viruses, worms, Trojan Horses and logic bombs.

Phishing is a digital form of social engineering that uses bogus emails that appear valid in order to request data from someone or point them to a replica website that then requests the data. Passive wiretapping is the observing or tracking of information, such as passwords transmitted unencrypted, while being sent over a communications link without disturbing or changing the information. Spamming is sending unsolicited email advertising for services, products and websites used as a delivery mechanism for malware and other cyber threats. Spoofing is generating a fake website to impersonate a real website run by a different party. Email spoofing

is altering the sender address and other parts of the email to appear as though the email came from a different source.

Structured Query Language (SQL) injection is an attack that involves the alteration of a database search in a web-based application; this is useful to obtain unauthorized access to sensitive information in a database. War driving is the act of physically driving around with a wireless-equipped device, probing for an unsecured wireless network. Once someone has gained access, any number of other exploits could follow. Lastly, zero-day exploits take benefit from formerly unidentified security weaknesses. By scripting an exploit for a formerly unidentified weakness, the attacker produces a superior threat since the compacted timeframe between public unearthing of both makes it problematic to guard against.

Statistics

Most of the cyberattack data on federal systems is not made available to the public; details such as what systems were attacked, what, if any, critical or sensitive data was compromised, or if those systems were rendered wholly inoperative. However, statistics on the level of cyber threats that the federal government is facing on a daily basis can provide some ideas on what the DOD must face. Figure 1 below shows the types of IS occurrences that occurred in fiscal year 2014. This figure supports the previously provided data on common types of exploits. As it stands, these numbers are expected to continue to rise each year unless federal agencies ensure that appropriate steps are taken to secure systems and information.

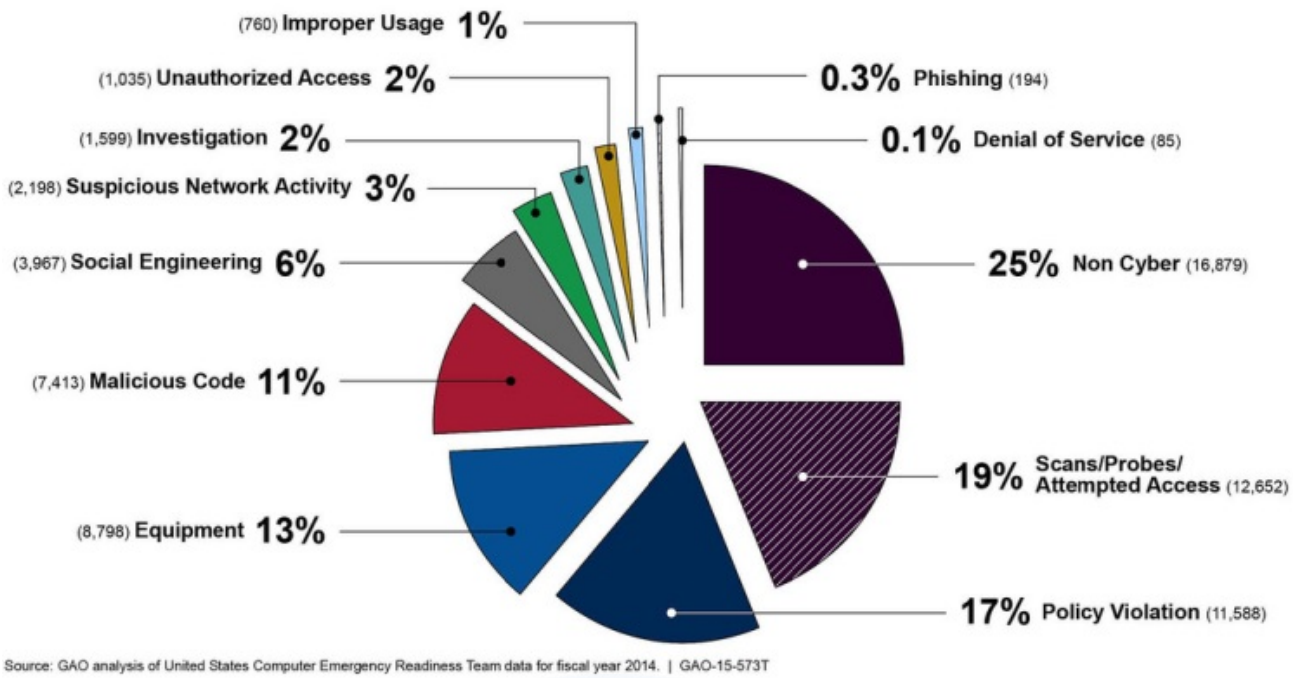

Figure 1: Information Security Incidents by Category for Fiscal Year 2014[12]

Commercial and Industry Involvement

It should come as no surprise that the DOD has in the past relied heavily on private sector innovation as the foundation for many of its capabilities. This holds true for some of the cyber security capabilities in place today. However, most commercial sector research and development of cyber protection technologies is driven by private sector needs and not DOD mission requirements; the commercial industry is primarily driven by profit and this drives the trade-off they will make to ensure the hardware and software in their manufacturing supply chains are free from viruses, back doors, and covert communications channels.[13] Although these steps are taken to ensure that commercial needs are met, their standards are usually not as stringent as those that are required by government agencies. Cybersecurity standards for industry must be put in place by the DOD for any components used in critical systems and networks. The DOD must ensure

that their cyber security requirements are well understood and known to commercial industry. The inherent problem lies with the rapid advancement of technologies, and the associated rapidly emerging requirements. It is increasingly important for the DOD to find a workable mix of GOTS and COTS to satisfy these requirements. Relying on just one or the other results in systems and networks that are vulnerable to cyberattacks; this is due to inherent security vulnerabilities that are not considered or are inherent to the system.

2011 DOD CYBER STRATEGY

This section turns to an analysis and critique of the 2011 Cyber Security strategy. It starts by briefly reviewing the five strategic initiatives in order to give insight into important considerations for cybersecurity in 2011. It then discusses the strengths and opportunities as well as its weaknesses and oversights. An analysis shows that although the DOD was on the right track with its initiatives, additional considerations necessary to fully combat the cybersecurity threats are not present. This information provides a basis for the improvements that the 2015 DOD cyber strategy contains. It is important to note that some aspects of these strategic initiatives overlap with each other; in order to achieve the goals set forth; there are common actions deemed necessary for this cyber security strategy.

Strategic Initiatives[14]

Strategic Initiative 1: DOD will treat cyberspace as an operational domain to organize, train, and equip so that DOD can take full advantage of cyberspace's potential.

Cyberspace is different from other DOD domains in that it is not a physical domain; it is a man-made domain created when computers, switches, routers, fiber optic cables, wireless

devices, satellites and other components are connected to allow for the movement of large amounts of data at fast speeds. This initiative proposed that the DOD must treat it the same as the other domains so that it used to support those domains; this led to the establishment of USCYBERCOM. Planned activities include integrating cyberspace scenarios into existing training and exercise, as well as developing increasingly resilient networks and systems for contingency purposes.

Strategic Initiative 2: DOD will employ new defense operating concepts to protect DOD networks and systems.

Proposed concepts under this initiative included the DOD enhancing its cyber hygiene best practices; discouraging and reducing insider threats by solidifying workforce communications, responsibility, internal observation and information management competencies; commissioning active cyber capabilities to avert intrusions onto networks and systems; and evolving new operational defense capabilities and architectures.

Strategic Initiative 3: DOD will partner with other U.S. government departments and agencies and the private sector to enable a whole-of-government cybersecurity strategy.

This initiative proposed that the DOD should work with DHS, other federal agencies, and the private sector to promote sharing of ideas, development of novel capabilities, and backing of cooperative efforts. Both the Secretary of Defense and Secretary of Homeland Security in order to align and improve cybersecurity collaboration signed a 2010 memorandum of agreement. This memo stated that there is a formalized structure to reaffirm the limits that current law and policy set on DOD and DHS collaboration, and to introduce joint participation in program planning to

increase each department's mission effectiveness.[15] DOD also planned on supporting DHS in leading interagency efforts to identify and mitigate cyber vulnerabilities in critical infrastructures.

Strategic Initiative 4: DOD will build robust relationships with U.S. allies and international partners to strengthen collective cybersecurity.

This initiative focused on supporting the U.S. *International Strategy for Cyberspace* by working in association with other government agencies to form healthy international relationships to echo core obligations and mutual interests in cyberspace. DOD would support efforts to spread the improvement and elevation of international cyberspace norms and ideologies that encourage candidness, security, dependability and interoperability. An additional part of this initiative was to encourage responsible behavior and oppose those who would seek to disrupt networks and systems, and to develop collective self-defense and increase collective deterrence.

Strategic Initiative 5: DOD will leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation.

This initiative focused on leveraging scientific, academic, and economic assets to foster a team of gifted civilian and military personnel to function in cyberspace and realize goals. Key factors included investing and in people, technology, and research and development; the idea was to evaluate the cyber personnel, requirements and capabilities on a systematic basis. This initiative also stated that it would encourage private sector participation in the development of robust cyberspace capabilities.

Strengths and opportunities

Considering that this is the first cyber strategy written by the DOD, it has a number of strengths and opportunities. It was released two years before the Cyberspace Operations Joint Publication, and is credited with providing a foundation for that doctrine. It also promoted a general awareness to the rising concern of an increase of cyber security incidents.

The strongest initiative is the first one, treating cyberspace as an operational domain. By giving it the same credibility and visibility as the other domains, it allows for an alignment of budget, training and equipment to fully realize the other initiatives. Standing up USCYBERCOM as a sub-unified command of USSTRATCOM demonstrated that the DOD is dedicated to efficiently and effectively organizing its resources to support the mission.

This cyber strategy introduced the central aspects of key cyber threat; these include external threat actors, insider threats, supply chain vulnerabilities, and threats to DODs operational ability.[16]Although the methods to deal with these threats are different today, the early identification of them allowed for gathering data useful to further modify how to combat the threats at the time of writing and in the future. It showed that the DOD has a good grasp of the cyber threats, even if there were not suitable capabilities to combat them.

Another strength of this cyber strategy is the introduction of active cyber defense capabilities. It defines active cyber defense as the DOD's synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities.[17] Although early in its conception, this concept paves the way for the distinction between defensive and offensive cyber defense capabilities seen and expanded on in the 2015 cyber strategy.

Additionally, the strategy recognizes the significance of collaboration between the DOD, other government agencies, and allied nations. By proposing to seek increasingly robust relationships between those with common interests and commitments, it shows recognition that no single entity can maintain effective cyber defenses on its own. It suggests plans such as joint training activities, developing shared warning systems, and sharing the burden of developing capabilities that benefit all interested players.

This strategy also emphasized an importance on ensuring that the cyber workforce is attracting the right talent and ingenuity needed to make the other strategic initiatives a reality. It proposes using a Presidential Initiative to attract new people and improve the federal recruitment and hiring process. It also concedes to the need for rapidly advancing technology, offering a streamlined approach. The 2011 DOD cyber strategy proposed adopting a five principle method for the DOD acquisition process for information technology related products. Logically, the principles made sense; making speed a critical priority, employ critical incremental development and testing rather than a single deployment of a complex system, willingness to sacrifice or defer some customization to achieve speedy incremental improvements, having information technology needs adopt differing levels of oversight based on the DIDs prioritization of critical systems, and improving security measures taken with all of the systems purchased by the DOD.[18]

Weaknesses and oversights

The 2011 cybersecurity strategy was well intentioned, but some of the strengths highlighted above are also weaknesses due to the vague nature and lack of feasible enforcement of the initiatives. The strategy reads as a statement from the government about the strategies and plans that are already in progress, and doesn't promote additional measures to take.

From an introductory perspective, no primary mission is identified. The strategy weakly described the current cyber posture and its strengths and opportunities in cyberspace, as well as the known threats. Without a primary mission set forth, the strategic initiatives had no mission goals to directly address, forcing the strategy to appear unfocused. The strategy does not directly state why the five initiatives are important to the overall DOD cyber mission.

The strategy proposed an accelerated acquisition process to reduce the amount of time to buy new technology from seven or eight years to a cycle of 12 to 36 months.[19] It is a move in the right direction, however 12 months is still too long to purchase and implement a cyber security infrastructure; the DOD needs to react in days and weeks, not in terms of months, years and decades.[20] Compared to the commercial sector and even other countries, a 12 to 36 month acquisition process is entirely too cumbersome to keep up with the rapidly advancing technologies that adversaries have at their disposal. By sacrificing or deferring customization to achieve faster incremental improvements, the DOD exposes itself to a reliance on COTS systems that are more susceptible to compromise through poor SCRM practices.

In terms of employing new defense operating concepts to protect DOD networks and systems, the strategy is not specific about what capabilities it will invest in, and how to take advantage of them. The strategy states that the DOD would enhance its cyber hygiene best practices, but that is all they are – best practices. By merely suggesting the minimum standards and not addressing anything further, it does read as impactful. It also fails to clarify the influence that the human element has and how the strategy will directly deter insider attacks. The strategy makes an effort to promote the concept of active cyber defense capabilities with real time detection and prevention of intrusion, but does not explicitly say how it is accomplished, or who

will provide the technology. It also does not state why it is useful to detect, discover, map and mitigate malicious activity on DOD networks.[21]

Although the cyber strategy mentions the addition of active cyber defense capabilities, the strategy as a whole focuses mostly on defensive protection of networks and systems, and does not endorse the need for offensive cyber defense capabilities. Emphasizing a defensive stance towards cyber security instead of both a defensive and an offensive stance promotes the illusion that defensive capabilities alone are enough to combat the current and future cyber threats.

Lastly, and perhaps most importantly, the strategy made no mention of the necessity for attribution to the attacks, such as those that are highest in number or pose the biggest threats. No clear distinction between the different types of adversaries was made; nor does it address their ingenuity in devising ways to obfuscate attribution. The strategic initiatives did not include any attribution plans to track and collect data on attacks, both in who was behind them, the motives, and methods used. Although this information would have been classified, the strategy should have stated the intent to use this data to deter future cyber events from occurring.

2015 DOD CYBER STRATEGY

This section covers the 2015 DOD Cyber Strategy. As it becomes apparent, the 2015 DOD cyber strategy contains significant improvements over the 2011 DOD cyber strategy; there is evidence in the details alone (19 pages for the 2011 strategy, 42 pages in the 2015 strategy). The 2015 DOD cyber strategy contains many of the same initiatives as the 2011, aimed at directly supporting primary missions identified prior to introducing the newly revised strategic

goal. The primary missions that the 2015 DOD cyber strategy sets forth are summarized below, followed by the strategic goals employed to satisfy those mission requirements.

Primary Missions[22]

First Primary Mission: The DOD must defend its own networks, systems, and information.

In support of cyberspace recognition as an operational domain, the DOD has a duty to protect its own systems against attack and rapidly recuperate if security methods fail. This also includes being able to operate in an environment where access to cyberspace is contested; the DOD must carry out its missions to secure the U.S. and learn to function without the implements that have become a critical part of everyday lives and operations.

Second Primary Mission: The DOD must be prepared to defend the United States and its interests against cyberattacks of significant consequence.

Significant consequences include mass casualties, large-scale destruction to property, crucial adverse U.S. foreign policy penalties, or severe economic impact on the U.S. To this end, if ordered by the President, the U.S. military may conduct cyber operations to neutralize a looming or on-going attack against the U.S. homeland or U.S. assets in cyberspace. The U.S. will pursue to deplete all network defense and law enforcement choices to lessen any potential cyber risk before conducting cyberspace operations.

Third Primary Mission: If directed by the President or the Secretary of Defense, DOD must be able to provide integrated cyber capabilities to support military operations and contingency plans.

To ensure that the Internet remains open and secure, the U.S. will always undergo cyber operations under a principle of limitation, as obligated to defend human lives and to avert the devastation of property. Similar to the other domains, the DOD will continuously perform in a

way that mirrors lasting U.S. values; any choice to conduct cyber operations external to DOD networks adheres to strict policy oversight and in accord with all conflict laws.

Strategic Goals[23]

Strategic Goal I: Build and maintain ready forces and capabilities to conduct cyberspace operations.

To operate successfully in cyberspace, the DOD needs forces and employees that are proficient to the uppermost standard, prepared, and fortified with the finest technical capabilities. To take advantage of the investment that the DOD put towards the cyber workforce and technologies, the DOD must train its individuals, shape efficient organizations and command and control systems, and wholly grow the mandatory capabilities. This strategy sets precise goals for the DOD to meet as it hires, trains, and provides equipment for its forces and personnel in the immediate and near future.

Strategic Goal II: Defend the DOD information network, secure DOD data, and mitigate risks to DOD missions.

While the DOD cannot protect all of its systems and networks against every invasion, the DOD must prioritize its critical networks and information so that it can conduct missions successfully. It essential that the DOD also accounts for operating inside an interrupted or degraded cyber setting if an attack is successful, or if parts of the infrastructure on which it depend on for operational and emergency plans are degraded. This goal also states that the DOD must be prepared to assist other government agencies in hardening U.S. networks and information against cyberattacks and reconnaissance.

Strategic Goal III: Be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyberattacks of significant consequence.

This goal states that the DOD must consult with other government agencies, private companies, and allied nations to discourage and stop a cyberattack of noteworthy magnitude on the U.S. The DOD must mature its intelligence, cautionary, and functioning capabilities to lessen refined and malevolent attacks; accomplished through constructing partnerships with interagency partners to conduct joint cyber operations to discourage and stop aggression in cyberspace.

Strategic Goal IV: Build and maintain viable cyber operations and plan to use these operations to control conflict escalation and to shape the conflict environment at all stages.

Through elevated tensions or absolute hostilities, the DOD must be able to offer the President a variety of possibilities for handling conflict escalation. If ordered the DOD will take advantage of cyber operations to disrupt an adversary's networks, infrastructure, and weapons; the means should minimalize casualties and damage to properties. To guarantee unity of effort, the DOD will empower combatant commands to design and complement cyber operations with dynamic operations across all domains of military operations.

Strategic Goal V: Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability.

In its global cyber assignation the DOD seeks to extend operational partnerships where suitable, and to pursue partnership capacities in cybersecurity and cyber defense. The DOD must elect to concentrate its partnership bulk initiatives on capacities where vital U.S. national interests are most critical; in addition to enduring partner capacity construction efforts in other areas, the DOD will concentrate global engagement on other countries such as the Middle East, the Asia-Pacific, and NATO allies. Through this strategy the DOD will continuously evaluate the global environment and mature groundbreaking partnerships to answer back to opportunities and developing trials.

Strengths and Opportunities

This version of the DOD cyber strategy contains significant improvements over the 2011 cyber strategy. It is a more comprehensive and detailed articulation of the previous strategy; this strategy shows that the DOD wants to obtain transparent about U.S. military doctrine, policy, roles, and missions in cyberspace both to better inform the public debate and expand declaratory policy for cyber conflict.[24] By identifying the three primary missions up-front, the strategy aims to directly address those missions through pointed goals that intertwine with each other. After identifying the goals, the stated missions trace back to them. This strategy also provides an updated cyber threat list that is more inclusive than the previous strategy; it shows that the DOD has a better grasp of the key cyber threats. However, it does leave out one critical threat, supply chain, which is a discussion later with further detail.

An emphasis on attribution is included in this strategy. The DOD realized that anonymity allowed for state and non-state actors to pose cyber threats without fear of attribution or retaliation, leading to an increase of cyber-attacks. Adversaries who would otherwise abstain from conducting cyber-attacks have taken advantage of resources that would permit anonymity; this has caused an increase in attempts, knowing that it could not, or would not trace back to the source. As such, this strategy proposed an increase partnership with the intelligence community to unmask an actor's cyber persona, identify the attack's point of origin, and determine tactics, techniques and procedures.[25] Collecting and knowing this critical information could play an important role in dissuading cyber actors from conducting attacks in the first place.

A dominant intention of this strategy was to set precise aims and objectives to dictate the creation of a Cyber Mission Force (CMF) of cyber personnel and forces. The CMF is comprised

of three teams and aligned as follows: Cyber Protection Forces would supplement traditional defensive procedures and defend important DOD networks and systems against significance threats; National Mission Forces and their accompanying support members would defend the US against cyberattacks of substantial consequence; and Combat Mission Forces and their accompanying support members would sustain combatant commands by producing combined cyberspace efforts in backing of operational plans and contingency operations.[26] As of today, the CMF has been implemented as Cyber Mission Teams (CMTs) and its components are labeled as Cyber Protection Teams (CPTs) and National Mission Teams (NMTs).

This strategy also introduces the addition of a deterrence element responsible for the deterrence of state and non-state actors from conducting cyber-attacks against the U.S. The strategy states that this will require cooperation from multiple government agencies; achievement is not through the articulation of cyber policies alone, but through declaratory procedures, considerable warnings and cautioning capabilities, defensive posture, efficient response measures, and the general resiliency of networks and systems. As deterrence is partially a function of perception, the strategy asserts that the United States is able to announce or show efficient response capabilities to discourage an adversary from commencing an attack; develop proficient defensive capabilities to repudiate a probable attack from being successful; and strengthen the overall resilience of U.S. systems to endure a likely attack if it breaches defenses.[27]

The overall organization of this strategy is an improvement over the 2011 DOD cyber strategy. The strategic goals are listed and briefly s, and then there are further details provided in the implementation objective section. One major critique of the 2011 DOD cyber strategy is that it did not explicitly explain how the DOD planned on achieving the strategic initiatives that it

proposed. The 2015 DOD cyber strategy however, attempts to lay out a specific plan for carrying out the proposed goals in order to meet the mission objectives. It includes plans such as the previously mentioned CMF, building the Joint Information Environment (JIE), and improving the effectiveness of the DOD Computer Network Defense Service Provider (CNDSP). An entire section is dedicated to how the DOD planned on managing the strategy, this includes improving cyber budgetary management as well as conducing end-to-end assessments of the DODs cyber capabilities.

Weaknesses and Oversights

Although the 2015 DOD cyber strategy shows significant improvements over the 2011 DOD cyber strategy, it still has some weaknesses and fails to recognize items that are of utmost importance to a successful cyber strategy. Once through the identification of shortfalls, the proposed updated strategy aims to address them.

To start, the strategy promotes a heavy emphasis on needing to protect the United States and its interests against cyberattacks of significant importance. Certainly the DOD needs to keep this in consideration; however the strategy promotes the image that it is only focusing on the big picture, and fails to show an interest in protecting less significant networks and systems from state and non-state actors who do not wish to cause significant damage, but merely intent to carry out smaller scale attacks. Collectively, these attacks could eventually lead to substantial loss if not prevented. For instance, the strategy suggests that the DOD should partner with the private sector to utilize their products and innovation for DOD cyber security purposes, but does not outline plans to assist these companies in their own cyber security missions. Rather, it simply

mentions that companies must prioritize what they consider significant enough to safeguard, and spend time and money in improving their own security.

As previously mentioned, the three biggest cyber threats to the U.S. are supply chain, malicious insiders, and foreign actors.[28] The strategy addresses goals to combat both malicious insiders and foreign actors, but makes no mention of how to combat supply chain issues. This is a massive oversight as supply chain related cyber-attacks have risen greatly over the years, and will continue to do so without some action on behalf of the DOD. If the DOD plans on developing and increasing partnerships with the private sector, it must acknowledge and address the current supply chain issues and propose a way forward to deal with them.

The strategy has a valid point that it must build and maintain ready forces to conduct cyberspace operations, but provides more guidance than specific implementation. It states that the DOD will build viable career paths and focus on improving civilian recruitment and retention, but does not say how apart from providing an opportunity for an advancement track with best-in-class opportunities to develop and succeed within the workforce.[29] Why would an Active Duty officer or a highly skilled civilian settle for a career with the DOD or other government agency when there are potential offers for extremely high pay and other enticing benefits within the private technology sector? If the DOD is serious about building and maintaining ready forces, competitiveness is key, not just with compensation but with job satisfaction, opportunities for training and professional development, and overall interest in the assignments.

Mitigation of risk is a common theme evident throughout the entire strategy. However, a specific cyber risk management plan is not identified. For example, assessing vulnerabilities and

weaknesses in DOD systems is not easy due to the large number of such systems; even given assessed levels of risk for all systems, decision-makers may find it challenging to prioritize risk mitigation efforts due to uncertainties about whether there is an attack on high risk systems and how the functionality of systems weighs on the ability to conduct missions. Cyber risk changes over time, with the discovery of vulnerabilities in new and upgraded systems; therefore the importance of conduction of risk assessments with sufficient regularity to keep up with the pace of change is vital.[30] Construction of a defined risk management plan specific to cyber security is necessary in order to properly mitigate all risk identified in the strategy.

RECOMMENDATIONS

The intent of this section is not to propose an entirely new cyber strategy; rather it is to build upon the existing strategy to allow the DOD to achieve an advantage against existing and near-term cyber threats. It will address the shortcomings that were identified in the previous cyber strategies and make recommendations for inclusions in the next revision of the DOD Cyber Strategy as well as why it is necessary. It is important to keep in mind that upcoming strategies should also be dynamic in nature, and open to further revisions as necessary.

Supply Chain

One glaring oversight in the 2015 DOD cyber strategy is the lack of acknowledgment of supply chain issues. Poor supply chain management leads to concerns such as hardware and software having covert communications channels, back doors and viruses. An inclusion of a strategic goal that addresses supply chain problems is necessary to ensure that there are no opportunities for adversaries to insert concealed functions.

To counter supply chain vulnerabilities, the DOD must gauge the level of trust in numerous components and understand the risk they pose to the execution of critical mission functions. A key element to developing trust is the ability to perform hardware and software analysis, automated reverse engineering and the advancement of threat avoidance metrics and modeling capabilities that will deliver an understanding of the comprehensive risks in complex mission systems.[31] The DOD must work closely with vendors that provide components and systems for cyber security; not only is there a necessity for a manageable balance of government and commercial off the shelf products, but supply chain verification and security at all levels is required. Something as simple as a virus inserted on a single chip on a large system could do significant damage to a critical infrastructure if not prevented. A higher level of supply chain assurance could also be achieved by increasing the supply of components produced domestically. The DOD should have better insight into domestic suppliers, as opposed to those that are located internationally; it could control the quality and authentic of all products through monitoring efforts and regulations.

By conducting these efforts to counter the supply chain vulnerabilities, the DOD would not only assure the integrity of critical systems and networks, but also deny adversaries multiple avenues in which they could compromise or cripple them. Ensuring that all critical systems and networks are comprised of secured supply chain components promotes a reliable and dependable cyber security environment.

Cyber Risk Management

The 2015 DOD cyber security strategy places a heavy emphasis on mitigating risk, but does not state why that is important or how it plans on doing so. The next revision of DOD cyber strategy must reference the Risk Management Framework (RMF) and identify its application to

cyber security.[32] As directed by Executive Order 13636, the National Institute of Standards and Technology (NIST) has developed a Cybersecurity Framework that is recommended for use by the DOD to apply the principles and best practices to reduce cyber risk while enhancing resiliency. The DOD cyber strategy should emphasize the use of the Cybersecurity Framework to provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help the DOD identify, assess, and manage cyber risk for critical infrastructures. [33]

When adding the reference to RMF to the next revision of the DOD cyber security strategy, it will automatically apply to other areas of the strategy, such as supply chain and rapid cyber acquisition. To ensure RMF accountability, the DOD must trace all risk mitigation activities.

Private Sector Accountability

The 2015 cyber strategy insinuates that the private sector must prioritize their data and networks for protection, and make investments in improving their own cybersecurity. The strategy also indicates that the DOD should work with the private sector to develop and use their solutions to protect DOD systems and networks. What the strategy does not include is how the relationship could work the other way, with the DOD not only assisting the private sector with cybersecurity but also enforcing it so that critical data and systems are not compromised. The current policy of voluntary regulation of cyber security is not adequate, especially considering that the private sector supplies and maintains much of the technology used by the DOD and other government agencies.

Not only can poor cyber defense in the private sector lead to the loss of trade secrets and proprietary information, but cyber-attacks can take a kinetic form, harming equipment and facilities of those attacked. According to a report from a cyber security firm, from 2006-2013, the Chinese People's Liberation Army had an army cyberattack unity compromise 141 companies spanning 20 major industries, from information technology and telecommunications to aerospace and energy, using a well-defined attack methodology, honed over years and designed to steal large volumes of valuable intellectual property.[34]

The DOD needs to partner with other government agencies (namely DHS) to establish clear standards for the private sector. One of the standards recommended for companies is a requirement to report all cyber security related incidents, regardless of the size or damage related to the breach. This information is beneficial for the government to track to analyze trends and learn how to assist in combating the threats.

All private companies should adhere to the NIST Framework standards, or at the very least meet a mandatory minimum set of cyber security standards. The DOD could adopt a reward or punishment system; award federal contracts to companies that have met baseline cyber security standards and encourage sanctions on private sector entities that have not adopted reasonable cyber security practices. This would encourage all private companies to invest in cyber security, to avoid a shut out by the largest possible contracts available. Most private companies view more government regulation and oversight as a burden that costs money and inhibits innovation; although increased regulation is more burdensome for these corporations, the lack of concrete cybersecurity standards in private industry are creating large vulnerabilities which could become a national security threat.

Rapid Cyber Acquisition

It is no secret that the traditional DOD acquisition process is exceedingly slow and cumbersome, with the amount of time to purchase new technology sometimes taking up to ten years and often times results in delivering cyber systems that are late-to-need or obsolete. With technology rapidly advancing at an increasingly faster rate, it is imperative that the DOD modify this archaic process to better suit the cyber security infrastructure, especially considering that adversaries with malicious intent are not limited by the same process of acquiring technology and can do so in a much timelier fashion.

The next revision of the DOD cyber strategy must reference and enforce the recent changes made to the Joint Capabilities Integration and Development Systems (JCIDS) requirements process. The variation allows for a Joint Requirements Oversight Council (JROC) to designate a suitable group as the sponsoring organization once the JROC approves an Information Systems-Initial Capabilities Development Document (IS-ICD), thus relieving the suitable group from having to return to JROC for endorsement of additional requirements unless those requirements surpass the recommended thresholds.[35]

To counter rapidly evolving cyber threats, the DOD must work directly with the cyber operational and acquisition communities to understand rapidly emerging requirements, address urgent needs, and streamline the development, test and transition process of cyber capabilities.[36] By restructuring the cyber acquisition and operations policy to a rapid cyber acquisition model, DOD can ensure a prompt and total insertion of new technologies to combat the existing and future cyber threats that evolve constantly.

Cyber Workforce

In order to fortify the cyber workforce, the DOD cyber strategy must lay out a specific implementation plan, instead of merely providing guidance. If the DOD cannot offer a unique and rewarding mission to offset the other competitive advantages that private industry can offer, it will continue to have an increasing problem with recruitment and retention of cyber warriors, which are described as individuals engaged in offensive and defensive cyber operations.[37]

As more and more universities and higher level institutions acknowledge that cyber security is a growing career field, they are offering advanced degrees and research opportunities aimed at directly providing a solid background necessary for an in-depth understanding of cyber security. Not only should the DOD look for civilians that have a strong technical background for recruitment, but a strong technical background is a necessary requirement for Active Duty officers. Modeling the career path for an Active Duty cyber warrior after the pilot program is another option. Cyber warriors should obtain undergraduate degrees in the cyber security, networking and/or computer science areas; followed by an intensive training program to include realistic simulated attacks and defense, after which tracking and documentation of operational hours related to cyber security indicates their expertise. An increased effort for Active Duty officers and civilians to go regularly to continued learning and new informational classes to stay current on trends and technological advances follows.

One of the largest issues with retaining cyber talent goes beyond the training pipelines. The training framework is good, but one can argue that the material that the officers are being trained is inadequate. Additionally, the big angst in cyber operations currently is how the officers and enlisted personnel are being used. They are typically doing normal maintenance activities

instead of actual attack and defense operations, and this is immensely boring. A lack of practice ranges and simulators does not let operators fully train new tactics, techniques, and procedures.

This proposed program will aid to keep the cyber warriors excited about their careers by providing them with a unique and rewarding mission. It will also assist the DOD in recruiting and retaining top talent normally hired by private companies offering better compensation. An employee must show that they have adequate advancement and growth opportunities to support a long term commitment to a mission. If a cyber warrior embraces a culture of training, education, exercises, continuous learning to evolve effective tactics, techniques and procedures, sound operational risk management, and routine evaluations of compliance and operational effectiveness then they will in return thrive on professional competency, discipline, innovation and teamwork, as well as a comprehensive knowledge of the application of Joint combat power.[38]

CONCLUSION

This paper began with an overview of the current DOD cyber posture. The overview included the current collaborative efforts in which DOD participates, as well as a brief description of some of the most critical threat types that are present today. Descriptions of common threat sources and types of exploits that are most typical followed. This section also provided some statistics on number of attacks and whom they affected.

The next sections consisted of an analysis and critique of both the 2011 and 2015 Cyber Security strategies. They started by briefly reviewing the primary missions, strategic initiatives

and strategic goals in order to give insight into important considerations for cybersecurity. They then discussed the strengths and opportunities as well as the weaknesses and oversights.

By providing a background on the current cyber posture and an analysis on the initial and current DOD Cyber Strategy, there are recommendations provided on further revisions to the current DOD cyber strategy to achieve an advantage against existing and near-term cyber threats. Recommendations included addressing supply chain threats and how to reduce the number of compromised components; guidance on how to provide assistance with private sector accountability with securing their own networks and systems follows. A suggestion that an adherence to both the NIST Cybersecurity Framework standards for risk mitigation as well as the updated JCIDS process for rapid cyber acquisition inclusion in the updated DOD cyber strategy is made. Lastly, an improved recruitment and retention process is proposed to grow a reliable cyber workforce that is dedicated to the cyber mission. With all these recommendations considered in the next revision of the DOD cyber strategy, it becomes a more robust strategy that will reflect aspects of the cyber posture that are not currently considered.

Although this is not a specific recommendation for something to add to the next revision of the DOD cyber strategy, it is important to mention the concept of a Cyber Force. There are many schools of thought that believe that sometime in the near future there should be the construction of a separate Cyber Force, instead of pulling and combining resources from multiple federal agencies. This thought has a lot of merit, supported by facts considered in this paper. A dedicated Cyber Force would allot for its own chain of command and budget considerations, potentially cutting down the amount of bureaucracy that is currently hindering the cyber acquisition process. As it stands, USCYBERCOM does not have its own budgetary powers and acquisition arm, so it relies on the individual services. If there is a realization of a Cyber Force, it

would have its own acquisition proficiency, and could bypass most of the traditional JCIDS processes to rapidly field cyber capabilities.

The proposal of the ideas and recommendations in this paper is relevant for the current cyber posture. However, it is important to remember that the cyber domain is rapidly fluctuating and advancing, and the key take away is to maintain a strategy that is dynamic to future changes to sustain and progress the capabilities needed to deal with current and emerging cyber threats. What is recommended in this paper may not be lesser or increasingly relevant in future years as the cyber posture matures and changes.

NOTES

[1] Cartwright, James E., *Joint Terminology for Cyberspace Operations,* Memorandum from the Vice Chairman of the Joint Chiefs of Staff, 2010.

[2] "Cyber Vision 2025". *United States Air Force Cyberspace Science and Technology Vision 2012-2025*, AF/ST TR 12-01, 13 December 2012.

[3] *Paper -based and cyber-related incidents reported by federal agencies.* United States Government Accountability Office Report to Congressional Committees, GAO-15-290 High-Risk Series An Update, February 2015, pg 241

[4] *The Department of Defense Cyber Strategy,* April 2015. Pg 3

[5] Clapper, James R., *Statement for the Record – Worldwide Cyber Threats,* House Permanent Select Committee on Intelligence, September 2015.

[6] Ibid.

[7] *Cyber Command Fact Sheet,* https://www.stratcom.mil/factsheets/2/Cyber_Command/, March 2015.

[8] *Cyber Threat Intelligence Integration Center Fact Sheet,* https://www.whitehouse.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center, February 25, 2015.

[9] "Cyber Vision 2025". *United States Air Force Cyberspace Science and Technology Vision 2012-2025*, AF/ST TR 12-01, 13 December 2012.

[10] United States Government Accountability Office. 2015. *Information Security Cyber Threats and Data Breaches Illustrate Need for Stronger Controls across Federal Agencies*. Testimony Before the Subcommittees on Research and Technology and Oversight, Committee on Science, Space, and Technology, House of Representatives, Washington D.C.: US GAO.

[11] Ibid.

[12] United States Government Accountability Office. 2015. *Information Security Cyber Threats and Data Breaches Illustrate Need for Stronger Controls across Federal Agencies*. Testimony Before the Subcommittees on Research and Technology and Oversight, Committee on Science, Space, and Technology, House of Representatives, Washington D.C.: US GAO.

[13] "Cyber Vision 2025". United States Air Force Cyberspace Science and Technology Vision 2012-2025, AF/ST TR 12-01, 13 December 2012.

[14] "Strategy for Operating in Cyberspace", U.S. Department of Defense, July 2011.

[15] Memorandum of Agreement Between The Department of Homeland Security and The Department of Defense Regarding Cybersecurity, October 2010. nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-037.pdf

[16] "Strategy for Operating in Cyberspace", U.S. Department of Defense, July 2011.

[17] Ibid.

[18] Ibid.

[19] Ibid.

[20] Hoffman, Stefanie. "Partners Wary of DOD Cyber Security Plan". CRN News.com, 21 July 2011.

[21] "Strategy for Operating in Cyberspace", U.S. Department of Defense, July 2011.

[22] *The Department of Defense Cyber Strategy*, April 2015.

[23] Ibid.

[24] Zheng, Denise E., *2015 DOD Cyber Strategy*, Center for Strategic and International Studies, April 2015.

[25] *The Department of Defense Cyber Strategy*, April 2015

[26] Ibid.

[27] Ibid.

[28] "Cyber Vision 2025". *United States Air Force Cyberspace Science and Technology Vision 2012-2025*, AF/ST TR 12-01, 13 December 2012.

[29] Ibid.

[30] Schmidt, Lara, *Perspective on 2015 DOD Cyber Strategy*, RAND Office of External Affairs, September 2015.

[31] "Cyber Vision 2025". United States Air Force Cyberspace Science and Technology Vision 2012-2025, AF/ST TR 12-01, 13 December 2012.

[32] Department of Defense, *Risk Management Framework (RMF) for DOD Information Technology (IT)*, DOD Instruction (DODI) 8510.01, March 2014.

[33] The White House, *Executive Order – Improving Critical Infrastructure Cybesecurity*, Office of the Press Secretary, February 2013.

[34] Mandiant, Exposing *one of China's Cyber Espionage Units*, 2013. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

[35] McFarland, Katrina, *Testimony Before the Senate Armed Services Committee Subcommittee on Readiness and Management Support Witness Statement of HON Katrina McFarland*, February 2014.

[36] "Cyber Vision 2025". *United States Air Force Cyberspace Science and Technology Vision 2012-2025*, AF/ST TR 12-01, 13 December 2012.

[37] Li, Jennifer J., Daugherty, Lindsay, *Training Cyber Warriors*, Support for Public Policy, Santa Monica: Rand Corporation, 2015.

[38] Office of the Secretary of Defense, *Department of Defense Cybersecurity Culture and Compliance Initiative*, September 2015.

BIBLIOGRAPHY

Cartwright, James E., *Joint Terminology for Cyberspace Operations*, Memorandum from the Vice Chairman of the Joint Chiefs of Staff, 2010.

Clapper, James R., *Statement for the Record – Worldwide Cyber Threats,* House Permanent Select Committee on Intelligence, September 2015.

"Cyber Vision 2025". *United States Air Force Cyberspace Science and Technology Vision 2012-2025,* AF/ST TR 12-01, 13 December 2012.

Cyber Command Fact Sheet, https://www.stratcom.mil/factsheets/2/Cyber_Command/, March 2015.

"Cyberspace Operations", *Joint Publication 3-12,* 5 February 2013.

Department of Defense, *Risk Management Framework (RMF) for DOD Information Technology (IT),* DOD Instruction (DODI) 8510.01, March 2014.

Hoffman, Stefanie. "Partners Wary of DOD Cyber Security Plan". CRN News.com, 21 July 2011.

Li, Jennifer J., Daugherty, Lindsay, *Training Cyber Warriors*, Support for Public Policy, Santa Monica: Rand Corporation, 2015.

Mandiant. *Exposing one of China's Cyber Espionage Units*. 2013 http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

McFarland, Katrina, *Testimony Before the Senate Armed Services Committee Subcommittee on Readiness and Management Support Witness Statement of HON* Katrina McFarland, February 2014.

Memorandum of Agreement Between The Department of Homeland Security and The Department of Defense Regarding Cybersecurity, October 2010. nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-037.pdf

Office of the Press Secretary, *Cyber Threat Intelligence Integration Center Fact Sheet,* https://www.whitehouse.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center, February 25, 2015.

Office of the Secretary of Defense, *Department of Defense Cybersecurity Culture and Compliance Initiative,* September 2015.

Paper -based and cyber-related incidents reported by federal agencies. United States Government Accountability Office Report to Congressional Committees, GAO-15-290 High-Risk Series An Update, February 2015, pg 241

Schmidt, Lara, *Perspective on 2015 DOD Cyber Strategy,* RAND Office of External Affairs, September 2015.

"Strategy for Operating in Cyberspace", U.S. Department of Defense, July 2011.

"The Department of Defense Cyber Strategy", April 2015.

The White House, *Executive Order – Improving Critical Infrastructure Cybersecurity,* Office of the Press Secretary, February 2013.

U.S. Department of Homeland Security, *Cyber Resilience Review,* Stakeholder Engagement and Critical Infrastructure Resilience.

U.S. Strategic Command, *Cyber Command Fact Sheet,* https://www.stratcom.mil/factsheets/2/Cyber_Command/, March 2015.

United States Government Accountability Office. 2015. *Information Security Cyber Threats and Data Breaches Illustrate Need for Stronger Controls across Federal Agencies.* Testimony Before the Subcommittees on Research and Technology and Oversight, Committee on Science, Space, and Technology, House of Representatives, Washington D.C.: US GAO.

Zheng, Denise. E., *2015 DOD Cyber Strategy,* Center for Strategic and International Studies, April 2015.